Releases copy of prepared statement for cybersecurity symposium

WASHINGTON, D.C. – Congresswoman Loretta Sanchez (CA-47) today delivered the following remarks at a cybersecurity symposium hosted by the U.S. Naval Institute and CACI International Inc., entitled: "The Cyber Threat to National Security – Countering Challenges to the Global Supply Chain." At the event, Rep. Sanchez and other Members of Congress were invited to discuss their strategies for securing America's cyber networks and combating hackers and other potential threats.

"Good Morning. I would like to first thank the U.S. Naval Institute and CACI for organizing this important symposium to discuss and share ideas on cybersecurity and how we can successfully address the challenges to the global supply chain. I would also like to thank all of you for taking time out of your busy schedule to focus on what I consider a high priority issue for the security of our nation as a whole.

"Cybersecurity is an issue I have been working on for a very long time, as a member of the House Armed Services Committee and as the Vice-Chair of the Homeland Security Committee. Currently, I have the honor of serving as the Chairwoman of the Subcommittee on Terrorism and Unconventional Threats and Capabilities (TUTC) of the House Armed Services Committee. This subcommittee oversees the military's cyber strategy and examines ways to better recognize the vulnerabilities and better protect information systems within the Department of Defense (DoD).

"Cyber threats in general have only recently received the attention they deserve, particularly within the defense community. However, DoD has taken significant steps to gain a better understanding of how to best maintain information assurance and determine the resources needed to fully protect its information networks. In the 2010 Quadrennial Defense Review (QDR), DoD put great emphasis on strengthening DoD's capabilities in cyberspace by developing a comprehensive approach to DoD operations in cyberspace, developing greater cyberspace expertise and awareness and enhancing partnerships with other agencies and governments.

"At DoD, there are more than 15,000 different computer networks which are operated across 4,000 military installations around the world, and we need to protect them all! However, we not

only need to protect these networks but we must also encourage greater coordination between the Department of Defense and its industries. We must ensure that all information that goes beyond the walls of the Pentagon is protected.

“DoD works with countless defense industries and these industries must be held responsible for handling all classified and unclassified information appropriately. Recently, DoD announced a proposal which would create a broad foundation for secure information sharing between DoD and its industries and ensure that industries handle sensitive material properly. I believe these are the types of proactive steps DoD needs to take in order to not only protect our weapons and information systems but also our military operations on the frontlines.

“Last week, my subcommittee held a hearing where we heard from the private sector about their perspectives on the Department of Defense information technology and cybersecurity activities and how we can better work with the private sector to improve the protection of our information systems. The committee discussed how there is an array of intellectual capital and expertise in the private sector that is not adequately consulted even though decisions will typically have as much of an impact on industry as it will on government.

“We also discussed how DoD needs to develop a solid response plan to a cyber attack along with focusing on long-term resources and solutions so that we are not constantly in a reactive state. The President’s Fiscal Year 2011 budget proposed an increase of more than $70 million for computer science and security research in the Science & Technology budget. I believe it is imperative for DoD to engage the private sector as they decide how to invest this new funding.

“There is an array of intellectual capital and expertise in the private sector that is not adequately consulted on key strategic questions. As I stated during the subcommittee hearing last week, we need to recognize that the private sector is very much part of the DoD family, and should be treated that way.

“There have been many discussions in the press regarding cybersecurity, in large part because of the hacking attacks on Google. However, the situation with Google was only one of many cyberattacks against the United States and U.S. companies.

“There have been a number of attacks specifically against DoD, including reports of intrusions

into contractor networks to infiltrate data on the F-35 Joint Strike Fighter, intrusions into the networks that control our electricity grid, and intrusions on Pentagon email networks. Without properly protecting our networks from all these different types of cyber threats, we put our supply lines and ultimately the lives of our troops at risk.

“And this is exactly why I am here today, along with all of you—because we not only recognize cyber threats as a top security issue but we also understand the urgency of the issue.

“I hope that today’s symposium is only the beginning of a long-term discussion about how to best protect this country’s information networks. Thank you again, for inviting me to participate on this distinguished panel and I look forward to you questions.”

# # #